AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Two (2) Subject Device: A BLU View 3 Cell Phone and a Samsung Galaxy A8 Table, more fully described in Attachment A.	)	Case No. MJ25-136

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
Two (2) Subject Device: A BLU View 3 Cell Phone and a Samsung Galaxy A8 Table, more fully described in Attachment A.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(2),(b)(2)	Possession of Child Pornography

The application is based on these facts:

✓ See Affidavit of FBI Special Agent Kelly H. Forest, continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Kelly H. Forest, Special Agent (FBI)
Printed name and title

◯ The foregoing affidavit was sworn to before me and signed in my presence, or
◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 03/14/2025

Judge's signature

City and state: Seattle, Washington

Paula L. McCandlis, United States Magistrate Judge
Printed name and title

USAO: 2025R00265

AFFIDAVIT OF SPECIAL AGENT KELLY FOREST

STATE OF WASHINGTON)
) ss
COUNTY OF SNOHOMISH)

I, Kelly Forest, a Special Agent with the Federal Bureau of Investigation (FBI), Seattle, Washington, having been duly sworn, state as follows:

AFFIANT BACKGROUND

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since 2020. I am a law enforcement officer of the United States, within the meaning of Title 18, United States Code, who is empowered by law to conduct investigations of, and to make arrests for offenses enumerated in Title 18, United States Code.

2. I am assigned to the Everett and Bellingham Resident Agency as part of the FBI's Seattle Field Office, where I specialize in Violent Crimes Against Children and Human Trafficking investigations occurring in Snohomish, Skagit, Whatcom, Island, and San Juan counties, which are situated in the Western District of Washington. I am assigned to the FBI Seattle's Crimes Against Children & Human Trafficking Task Force, which includes investigations of the online sexual exploitation of children involving the transmission, possession and production of child pornography, exploitation of children on the internet, and other federal criminal activity. I am also a member of the Seattle Internet Crimes Against Children Task Force ("Seattle ICAC"). The goal of the Seattle ICAC is to catch distributors of child sexual abuse material (CSAM) on the Internet, whether delivered on-line or solicited on-line and distributed through other channels and to catch sexual predators who solicit victims on the Internet through chat rooms, forums and other methods.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

3. During my career as an FBI Special Agent, I have served as the case agent in numerous child exploitation investigations. I have participated in all aspects of child exploitation investigations, including conducting surveillance, undercover operations, identifying victims, interviewing suspects, and executing arrest and search warrants. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications and executions, computer evidence identifications, computer evidence search and seizures, and various other criminal laws and procedures. I have received training regarding child pornography and child exploitation, and I have observed and reviewed examples of child pornography in various forms of media, including media stored on digital media storage devices.

4. As further detailed below, based on my investigation and the investigation of other law enforcement officers, I believe there is probable cause to conclude that a BLU View 3 cell phone and a Samsung Galaxy A8 Tablet (hereafter SUBJECT DIGITAL DEVICES) used by ROBERT ANTHONY FIORE, will contain evidence, fruits, and instrumentalities, of violations of Title 18 United States Code Sections 2252(a)(2),(b)(2) Possession of Child Pornography and 18 U.S.C. § 2252(a)(2) and (b)(1) Receipt or Distribution of Child Pornography.

5. The information contained in this affidavit consists of my personal knowledge gained through this investigation, information provided by other law enforcement officers involved in this investigation, information provided by witnesses and others with knowledge of the relevant events and circumstances, information gleaned from my review of evidence, and my training and experience. Because this affidavit is offered for the limited purpose of establishing probable cause, I list only those facts that I believe are necessary to support such a finding. I do not purport to list every fact known to me or others as a result of this investigation.

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

INTRODUCTION AND PURPOSE OF AFFIDAVIT

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to search the following SUBJECT DIGITAL DEVICES for evidence of violations of Title 18 United States Code Sections 2252(a)(4), (b)(2), Possession of Child Pornography and 18 U.S.C. § 2252(a)(2) and (b)(1) Receipt or Distribution of Child Pornography;

a. a BLU View 3 cell phone IMEI 353145920663719 (hereinafter SUBJECT DIGITAL DEVICE A);

b. a Samsung Galaxy A8 Tablet bearing S/N R9YT202ZF3N (hereinafter SUBJECT DIGITAL DEVICE B);

7. There is probable cause to believe the above-described SUBJECT DIGITAL DEVICES A and B used by ROBERT FIORE will contain evidence of this crime and contraband or fruits of this crime, as described in Attachment B.

DEFINITIONS

The following definitions apply to this affidavit:

8. "Chat," as used herein, refers to any kind of text communication over the internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as internet forums and email.

9. For the purposes of this affidavit, a "minor" refers to any person less than eighteen years of age and for the purpose of this search warrant, "Child pornography," as used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

10. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

11. "Cloud-based storage service," as used herein, refers to a publicly accessible, online storage provider that collectors of depictions of minors engaged in sexually explicit conduct can use to store and trade depictions of minors engaged in sexually explicit conduct in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders or collectors of depictions of minors engaged in sexually explicit conduct in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

12. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device," including smartphones and mobile devices.

13. "Data," as used herein refers to the quantities, characters, or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

14. "Digital Devices" as used herein refers to any physical object that has a computer, microcomputer, or hardware that is capable of receiving, storing, possessing, or potentially sending data.

15. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations, community-owned, non-profit, or otherwise privately-owned companies that are in business to provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

16. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

17. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

18. "User Attributes," as used herein refers to any tangible data, documents, settings, programs, or other information that provides information related to the identity of the specific user of the device, computer, application, program, or record.

INDIVIDUALS WITH A SEXUAL INTEREST IN MINORS

19. Based upon my knowledge, experience, and training in depictions of minors engaged in sexually explicit conduct investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals with a sexual interest in minors who are involved in depictions of minors engaged in sexually explicit conduct as described below.

20. Those who possess, receive and attempt to receive depictions of minors engaged in sexually explicit conduct may receive sexual gratification, stimulation, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity. As described herein, FIORE was in possession of child sexual abuse material (CSAM) and using Telegram to purchase CSAM. Based upon FIORES's 2021 conviction for Possession of Obscene Matter of Minor in Sexual Act coupled with his current state prosecution for Possession of Child Pornography and Dealing in Depictions of Minors Engaged in Sexually Explicit Conduct (based upon the conduct described below), there is ample evidence to confirm FIORE's sexualized interest in minors.

21. Those who possess, receive and attempt to receive depictions of minors engaged in sexually explicit conduct may keep records, to include names, contact information, and/or dates of their interaction, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

22. Those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly. Again, FIORE is a convicted sex offender who has maintained a sexualized interest in minors which he has cultivated by possessing depictions of minors engaged in sexually explicit conduct.

23. Those who possess, receive and attempt to receive depictions of minors engaged in sexually explicit conduct also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other depictions of minors engaged in sexually explicit conduct distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

contact and who share the same interests in depictions of minors engaged in sexually explicit conduct.

24. Those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct prefer not to be without their depictions of minors engaged in sexually explicit conduct for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of depictions of minors engaged in sexually explicit conduct throughout the world.

SUMMARY OF PROBABLE CAUSE

25. In February of 2025, Detective Sean Culbertson, Seattle Police Department (SPD), contacted the FBI regarding a Marysville Police Department (MPD) investigation into ROBERT ANTHONY FIORE. Detective Culbertson introduced me to MPD Detective Brandon Blake who was the assigned detective of the case. Detective Blake, a member of the Seattle Internet Crimes Against Children Task Force (ICAC), explained he received a Cybertip from the National Center for Missing and Exploited Children (NCMEC), reporting child sexual abuse material (CSAM) detected on a Dropbox user's account. Detective Blake provided me with the Cybertip and the returns from Dropbox, which I reviewed.

26. Based on my training and experience, I know that Electronic Service Providers ("ESPs") (e.g. Google, Meta, Snapchat, Yahoo) typically monitor their own services used by their subscribers. To prevent their communication networks from serving as conduits for illicit activity and pursuant to the terms of user agreements, ESPs routinely and systematically attempt to identify suspected depictions of minors engaged in sexually explicit conduct that may be sent through their facilities.

27. When the ESP detects such a file on its platform, the ESP reports that fact to NCMEC's CyberTipline. By statute, an ESP has a duty to report to NCMEC any apparent depictions of minors engaged in sexually explicit conduct it discovers "as soon

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

as reasonably possible." 18 U.S.C. § 2258A(a)(1). The CyberTipline report transmits the intercepted file from the ESP to NCMEC.

28. In the Cybertip submitted by Dropbox on October 11, 2024, CSAM was detected on a Dropbox user's account on October 10, 2024. Along with the report, Dropbox provided a video, which is described as follows:

a. A fully nude female child laying backside on a bed with her legs spread and vagina fully exposed. An adult female with brown hair begins to lick the child's vagina. The remainder of the video depicts the adult female performing oral sex on the child. At one point, the adult female repositioned the child's body closer to the camera. Based on the child's lack of pubic hair and breast development, and the size of her body compared to the adult female, I estimate her age to be between 7 and 11 years old.

I reviewed this file and believe it meets the federal definition of child pornography, as defined in 18 U.S.C. 2256(8).

29. Additionally, Dropbox provided the following name, email, and registration date and time for the account: Steve, stevelipshits@gmail.com, October 10, 2024 22:51:11 UTC. I noticed the registration date of the account was the same date Dropbox detected the CSAM.

30. On or around February 5, 2025, Detective Blake issued search warrants to Google for email address stevelipshits@gmail.com and to Comcast for the IP address associated with the Dropbox account at the time of registration, 2601:601:8303:4f80:4c69:efba:8849:8bdb. Detective Blake reviewed the records and identified the Google Pay customer name and address was Rob Fiore, XXXXX 25th Ave NE, apt MXXX.

31. The Comcast returns for the IP address associated with the Dropbox account on October 10, 2024 22:51:11 UTC resolved to address XXXXX 25th Ave NE,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

apt MXXX, Marysville, WA. This was the same address listed for the Google Pay customer address.

32. I reviewed the Google returns and identified numerous selfie-style photos of FIORE in the "photos" folder. I also observed a photo of a Washington State driver's license with the name Robert Anthony Fiore, date of birth (DOB) XX/XX/1970 and address XXXXX 25th Ave NE, apt MXXX, Marysville, WA. This is the same address associated with the Google Pay customer address and Comcast returns.

33. I reviewed FIORE's criminal history and saw that FIORE had a previous misdemeanor conviction for Possession of Obscene Matter of Minor in Sexual Act in 2021, and he is actively registered as a sex offender.

34. On February 14, 2025, I accompanied MPD and ICAC on a residential search warrant of FIORE's Marysville, Washington residence. According to Detective Blake's report, following advisement and waiver of his constitutional rights, FIORE confirmed he used email addresses robfiore@bellsouth.net and stevelipshits@gmail.com. He admitted to chatting with minors online for the last year, where the youngest person claimed to be 12 years old. He said he was chatting with more than a dozen people who claimed to be minors.

35. During the search, another ICAC detective showed me messages from FIORE's Telegram account. I noticed a conversation between FIORE and another Telegram user where they were discussing the price of CSAM. The other Telegram user sent FIORE screenshots of a Telegram channel named "legit teen cp group" with thumbnail images of CSAM and Mega file downloads. The other user then sent FIORE a Bitcoin wallet address, and FIORE responded with a screenshot of a Bitcoin transaction of approximately $50 USD to the same wallet address. The transaction took place on February 13, 2025. Additionally, on February 14, 2025, FIORE confessed to purchasing CSAM as recent as "last night," (February 13, 2025).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

36. MPD seized two digital devices during the execution of the residential search warrant at FIORE's apartment: one BLU View 3 cell phone IMEI 353145920663719 (SUBJECT DIGITAL DEVICE A) and one Samsung Galaxy A8 Tablet bearing S/N R9YT202ZF3N (SUBJECT DIGITAL DEVICE B). Based on my training and experience, neither SUBJECT DIGITAL DEVICE is manufactured in the State of Washington. The SUBJECT DIGITAL DEVICES are currently secured at FBI Seattle.

TECHNICAL BACKGROUND

37. Courts have recognized that the majority of Americans possess and use cellular telephones, and that most of those keep the phones within their reach at all times. Cellular telephones are used for, among other things, voice, text, email, and SMS communications; accessing and posting to social networking websites, surfing the internet, taking, and storing photographs, creating, and storing documents, notes, music, mapping directions to places, etc. Courts have recognized that these devices "smart phones" are essentially small computers with vast storage capacities. Information deleted by the user can be recovered, years after deletion, upon examination of a cell phone's data.

38. Based on my training and experience, I know that the development of computers and portable digital devices in general have revolutionized the way in which those who seek out depictions of minors engaged in sexually explicit conduct are able to obtain this material. Computers serve four basic functions in connection with depictions of minors engaged in sexually explicit conduct: production, communication, distribution, and storage. Additionally, I know that the computer's capability to store images in digital form makes it an ideal repository for depictions of minors engaged in sexually explicit conduct. The size of the electronic storage media (often referred to as a "hard drive") used in home computers has grown tremendously within the last several years. Hard

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

drives with the capacity of terabytes are not uncommon. These drives can store thousands of images and/or videos at a high resolution.

39. Based on my training and experience and information provided to me by electronic forensic detectives and agents, I know that data can quickly and easily be transferred from one digital device to another digital device via messages, apps, file sharing etc., and via a USB cable or other wired connection. Data can be transferred from computers or other digital devices to internal and/or external hard drives, tablets, mobile phones, and other mobile devices via a USB cable or other wired connection. Data can also be transferred between computers and digital devices by copying data to small, portable data storage devices including USB (often referred to as "thumb") drives, memory cards (Compact Flash, SD, microSD, etc.) and memory card readers, and optical discs (CDs/DVDs).

40. Based on my training and experience, collectors and distributors of depictions of minors engaged in sexually explicit conduct also use online, remote, resources to retrieve and store depictions of minors engaged in sexually explicit conduct, including services offered by companies such as Google, Yahoo, Apple, Amazon, and Dropbox, among others. The online services allow a user to set up an account with a remote computing service that provides email services and/or electronic storage of electronic files in any variety of formats. A user can set up, and access, an online storage account from any digital device with access to the Internet. Evidence of such online storage of depictions of minors engaged in sexually explicit conduct is often located on the user's computer or smart phone.

41. Based on my training and experience, communications by way of a computer/smart device can be saved or stored on the computer/smart device used for these purposes. Storing this information can be intentional, i.e., by saving an email or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). Examples of this stored data include user-created or saved data, such as contact lists, messages sent and received, images, audio and video files, personal calendars, notes, prescriptions, bank statements, videos, documents, and images; as well as device-generated data, such as user identity information, passwords, usage logs and information pertaining to the physical location of the device over time. Examples of data stored in a smart phone that can reveal a person's location at specific dates and times include metadata and EXIF tags associated with photographs; IP addresses, which are associated with a geographic location; and geographic location associated with the phone sending/receiving signals with cell towers and satellites. As such, a person's use of the smart phone can reveal where a person has been at dates and times relevant to the crime(s) under investigation; a person's activity at relevant dates and times, and/or places a person frequents at which that person is likely to be found for arrest or at which the suspect stored or inadvertently left evidence behind.

42. In addition to electronic communications, a user's Internet activities generally leave traces or "footprints" and history files of the browser application used. A forensic examiner often can recover evidence suggesting whether a computer/smart device was using a specific website or application, and when certain files under investigation were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data. Additionally, even if such information is deleted from the memory or storage of the device the data may reside on the device for an extended period of time until overwritten by the operating system of the device.

43. Based on my training and experience, I have learned that in addition to the traditional collector, law enforcement has encountered offenders who obtain depictions of minors engaged in sexually explicit conduct from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a "seek and delete" offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification.

44. Based on my training and experience and my consultation with electronic forensic detectives and agents who are familiar with searches of computers and smart devices, I have learned that regardless of whether a person discards or collects depictions of minors engaged in sexually explicit conduct he accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be located. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of depictions of minors engaged in sexually explicit conduct, and other electronic artifacts that may be forensically recoverable.

45. Based on my training and experience and my consultation with electronic forensic detectives who are familiar with searches of smart devices, I have learned that offenders will try and obfuscate data containing images and videos of minors engaged in sexual activity. One potential manner of trying to hide the contraband may be by changing file extensions. For example, an image file may often have a file extension of ".jpg" of ".jpeg" signifying that it is an image or photograph. An offender may change the file extension by selecting the "save as" format on a computer or digital device and select ".doc" or ".docx" to make it appear that instead of a contraband image or photograph, it is a word document. The same process may be used to attempt to hide a video file as well. Based on these and other attempts to hide potential contraband, it is necessary for forensic examiners to examine all potential data on the computer.

46. Whether some data on the phone is evidence may depend on other information stored on the computer, and the application of an examiner's knowledge about how a computer operates. Therefore, the context, location, and data surrounding

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information in the computer's data may be necessary to understand whether evidence falls within the scope of the warrant.

47. I also know based on my training and experience that obtaining subscriber information for a particular device is often useful in determining who possessed the device on a particular date and time. However, a more definitive way to determine the possessor of a device is to examine how the device is used over a period of days or weeks. The content on the device itself, over a period of time, provides vital evidence of the identity of the user of the device; such evidence can be found in communication content, email information, linked social media accounts, photos (selfies), video, and any location data on the device. Examination of all this data is necessary to accurately determine who possessed the device at dates and times critical to the investigation.

48. I also know based on my training and experience that a search of the digital device itself would irreversibly alter data and/or evidence on the device. The commonly accepted best practice method to search a digital device for evidence involves creating a digital image of the device and then searching that image for the responsive evidence. Creating a forensic image does not alter any evidence on the device; it only copies the data into a searchable format. The image is then searched using search tools to locate and identify that evidence whose seizure is authorized by this warrant. The unaltered device and the image are then preserved in evidence.

49. As set forth herein, I seek permission to search for and seize evidence, fruits, and instrumentalities of the above-referenced crimes, and or things or data identifying the individual engaged in the above referenced criminal activity, that might be found in the SUBJECT DIGITAL DEVICES A and B, in whatever form they are found. It has been my experience that individuals involved and interested in depictions of minors engaged in sexually explicit conduct often prefer to store images or videos depicting depictions of minors engaged in sexually explicit conduct in electronic form. The ability to store images of depictions of minors engaged in sexually explicit conduct in electronic

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

form makes digital devices an ideal repository for depictions of minors engaged in sexually explicit conduct.

CONCLUSION

50. The affidavit and application are being presented by reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).

51. Based on the information set forth herein, there is probable cause to search the above-described SUBJECT DIGITAL DEVICES A and B, as further described in Attachment A, for evidence, fruits, and instrumentalities, of violations of Title 18 United States Code Sections 2252(a)(2),(b)(2) Possession of Child Pornography as further described in Attachment B.

KELLY H. FOREST
Special Agent
Federal Bureau of Investigation

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone on this 14th day of March, 2025.

THE HON. PAULA M. MCCANDLIS
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Property to Be Searched

This warrant authorizes the seizure and search of SUBJECT DIGITAL DEVICES:

a. SUBJECT DEVICE A: BLU View 3 cell phone IMEI 353145920663719;

b. SUBJECT DEVICE B: a Samsung Galaxy A8 Tablet bearing S/N R9YT202ZF3N;

and any other electronic storage media found therein the device including internal storage device cards which are currently located at the Seattle Federal Bureau of Investigation's secure evidence section.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Particular Things to be Seized

The following items, which constitute fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2) Possession of Child Pornography and 18 U.S.C. § 2252(a)(2) and (b)(1) Receipt or Distribution of Child Pornography, including:

1. All records on the SUBJECT DIGITAL DEVICES described in Attachment A that relate to violations of Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2), including:

a. Evidence of other accounts associated with this device including email addresses, social media accounts, messaging "app" accounts, payment apps, and other accounts that may be accessed through the digital device that will aid in determining the possessor/user of the device;

b. Evidence of use of the device to communicate with other individuals with a sexualized interest in minors or others about the above-listed crime(s), via incoming or outgoing calls, chat sessions, instant messages, text messages, app communications, social media, SMS communications, payments, and other similar digital communications related to the sexual abuse of a minor or the possession, receipt/distribution, and production of depictions of minors engaged in sexually explicit conduct;

c. Evidence of the identity of the person in possession of the device on or about any times that items of evidentiary value (user attribution evidence), located pursuant to this warrant, were created modified, accessed, or otherwise manipulated. Such evidence may be found in digital communications, photos and video and associated metadata, documents, social media activity, and electronically stored information from the digital device necessary to understand how the digital device was used, the purpose of its use, who used it, and when;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. Child pornography as defined in 18 U.S.C. § 2256 meaning any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), in any format or media;

e. Evidence of malware that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

f. Evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence, and/or evidence that any of the digital devices were attached to any other digital device;

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;

h. Evidence of times the digital device was used;

i. Electronically stored information from the SUBJECT DIGITAL DEVICES necessary to understand how the digital device was used, the purpose of its use, who used it, and when; and

j. Information that can be used to calculate the position of the SUBJECT DEVICES, including location data; cell tower usage; GPS satellite data; GPS coordinates for routes and destination queries between the above-listed dates; "app" data or usage information and related location information; and images created, accessed or modified between the above-listed dates, together with their metadata and EXIF tags.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970